CONNECTION TECHNOLOGY SYSTEMS

HET-3105-PLUS SERIES

Gigabit Ethernet 4-Port 10/100/1000Base-T with 1-Port 1000Base-X or 100/1000Base-X Uplink Managed CPE Switch

Network Management

User's Manual

Version 0.91

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc.
Contents subject to revise without prior notice.
All other trademarks remain the property of their owners.

Copyright Statement

Copyright © Connection Technology Systems Inc.
This publication may not be reproduced as a whole or in part, in any way whatsoever unless prior consent has been obtained from Connection Technology Systems Inc.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limitations are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if no installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into a different outlet from that the receiver is connected.
- Consult your local distributors or an experienced radio/TV technician for help.
- Shielded interface cables must be used in order to comply with emission limits.

Changes or modifications to the equipment, which are not approved by the party responsible for compliance, could affect the user's authority to operate the equipment.

Copyright © 2010 All Rights Reserved.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:
All trade names and trademarks are the properties of their respective companies.

Table of Content

1. INTRODUCTION 5
1.1 Interfaces 5
1.2 Management Preparations 6
1.3 LED Definitions 7
2. Command Line Interface (CLI) 8
2.1 Remote Console Management-Telnet 8
2.2 Navigating CLI 9
2.2.1 General Commands 9
2.2.2 Quick Keys 10
2.2.3 Command Format 10
2.2.4 Login Username & Password 12
2.3 User Mode 13
2.3.1 Ping command 13
2.4 Privileged mode 14
2.4.1 Copy-cfg command 14
2.4.2 Firmware command 15
2.4.3 Ping command 16
2.4.4 Reload command 16
2.4.5 Write command 16
2.4.6 Configure command 16
2.5 Configuration mode 17
2.5.1 Entering Interface Numbers 17
2.5.2 No command 18
2.5.3 Show command 18
2.5.4 Interface command 20
2.5.5 IP command 21
2.5.6 MAC command 23
2.5.7 QoS command 24
2.5.8 SNMP-Server command 27
2.5.9 Switch-info command 30
2.5.10 User command 31
2.5.11 VLAN command 32

2.5.12 Show sfp command 34
APPENDIX A: Set Up DHCP Auto-Provisioning 35

1. INTRODUCTION

Thank you for using the 4-Port 10/100/1000 Base-T plus 1-Port 1000 Base-X or 100/100 Base-T Fast Ethernet Smart Switch. The built-in management module allows users to configure this Smart Switch and monitor the operation status locally or remotely through network.

The Smart Switch is fully compliant with IEEE 802.3 and 802.3u standards. By employing store and forward switching mechanism, the Smart Switch provides low latency and faster data transmission. Moreover, it also supports more advanced functions such as QoS, VLAN, IGMP Snooping, etc. Users can configure the required settings of the Smart Switch and monitor its real-time operational status via Command Line Interface (CLI). For detailed descriptions on CLI, please refer to Section 2.

1.1 Interfaces

Figure 1 below displays the interface with four 10/100/1000Mbps LAN ports.

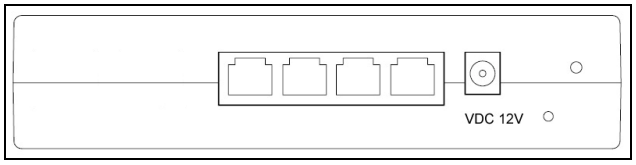


Figure 1. Four 10/100/1000 LAN Ports

Figure 2 below shows the top panel of the Smart Switch that displays LED indicators for each LAN connection and link status.

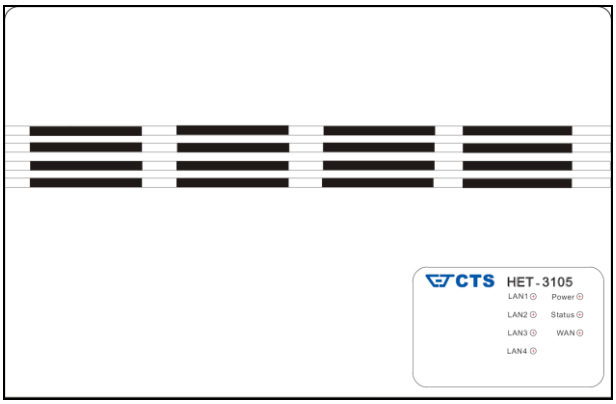


Figure 2. Top Panel with LED Indicators

1.2 Management Preparations

The Smart Switch can be accessed through Telnet connection. Before you can access the Smart Switch to configure it, you need to connect cables properly.

Connecting the Smart Switch

It is extremely important that proper cables are used with correct pin arrangements when connecting Smart Switch to other devices such as switches, hubs, workstations, etc.

1000Base-X / 100Base-FX SFP Port

The small form-factor pluggable (SFP) is a compact optical transceiver used in optical data communications applications. It interfaces with a network device mother board (for a switch, router or similar device) to a fiber optic or unshielded twisted pair networking cable. It is a popular industry format supported by several fiber optic component vendors.

SFP transceivers are available with a variety of different transmitter and receiver types, allowing users to select the appropriate transceiver for each link to provide the required optical reach over the available optical fiber type. SFP transceivers are also available with a "copper" cable interface, allowing a host device designed primarily for optical fiber communications to also communicate over unshielded twisted pair networking cable.

SFP slot for 3.3V mini GBIC module supports hot swappable SFP fiber transceiver. Before connecting other switches, workstation or media converter, make sure both sides of the SFP transfer are with the same media type, for example, 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX. In addition to that, check the fiber-optic cable type match the SFP transfer model. To connect to 1000Base-SX transceiver, use the multi-mode fiber cable that one side must be male duplex LC connector type. To connect to 1000Base-LX transfer, use the single-mode fiber cable that one side must be male duplex LC connector type.

1000Base-X Fiber Port

1000Base-X Fiber port is located inside the Smart Switch. This port is primarily used for up-link connection and will always operate at 1000M / Full Duplex mode. Duplex SC or WDM Simplex SC types of connectors are available. Use proper multimode or single-mode optical fiber to connect this port with other Gigabit Ethernet Fiber port. Before connect the other switches, workstation or Media Converter, make sure both side of the fiber transfer are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX. And check the fiber-optic cable type match the fiber transfer model. To connect to 1000Base-SX transfer, use the multi-mode fiber cable- with one side must be male duplex SC connector type. To connect to 1000Base-LX transfer, use the single-mode fiber cable-with one side must be male duplex SC connector type.

10/100/1000Base-T RJ-45 Auto-MDI/MDIX Port

Four 10/100/1000Base-T RJ-45 Auto-MDI/MDIX ports are located in front panel of the Smart Switch. These RJ-45 ports allow users to connect their traditional copper-based Ethernet/Fast Ethernet devices to the network and support auto-negotiation and MDI/MDIX auto-crossover. In other words, either crossover or straight through CAT-5E UTP or STP cable may be used.

Assigning IP Addresses

IP addresses have the format n.n.n.n, for example 168.168.8.100. IP addresses are made up of two parts:

- The first part (168.168.XXX.XXX in the example) refers as network address identifies the network on which the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network that wishes to connect to the Internet.

- The second part (XXX.XXX.8.100 in the example) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses allocated to you, consult the allocation organization from which your IP addresses were obtained.

Remember that no two devices on a network can have the same address. If you connect to the outside, you must change all the arbitrary IP addresses to comply with those you have been allocated by the allocation organization. If you do not do this, your outside communications will not operate.

A subnet mask is a filtering system for IP addresses. It allows you to further subdivide your network. You must use the proper subnet mask for proper operation of a network with subnets defined.

1.3 LED Definitions

LED	Color	Operation
Power	Off	System is power down.
	Green	System is power up.
Status	Green	System is working normally.
WAN	Off	Fiber link is down.
	Green	Fiber link is up and works in 100Mbps.
		Blinking when traffic is present.
	Orange	Fiber link is up and works in 1000Mbps.
		Blinking when traffic is present.
LAN1~LAN4	Off	LAN port link is down.
	Green	LAN port link is up and works in 100Mbps.
		Blinking when traffic is present.
	Orange	LAN port link is up and works in 1000Mbps.
		Blinking when traffic is present.

2. Command Line Interface (CLI)

This chapter introduces you how to use Command Line Interface (CLI) via Telnet connection, specifically in:

- Configuring the system
- Resetting the system
- Upgrading newly released firmware

2.1 Remote Console Management-Telnet

You can use Command Line Interface to manage the Smart Switch via Telnet session. For first-time users, you must first assign a unique IP address to the Smart Switch before you can manage it remotely. Use any one of the RJ-45 ports on the front panel as the temporary management console port to login to the Smart Switch with the default username & password and then assign the IP address using IP command in Global Configuration mode.

Follow steps described below to access the Smart Switch through Telnet session:

Step 1. Use any one of the RJ-45 ports as a temporary management console port to login to the Smart Switch.

Step 2. Run Telnet client and connect to *192.168.0.1*. For first-time users, make sure the IP address of your PC or workstation is assigned to an IP address between 192.168.0.2 and 192.168.0.254 with subnet mask 255.255.255.0.

Step 3. When asked for a username, enter "***admin***". When asked for a password, *leave the password field blank* and press Enter (by default, no password is required.)

Step 5. If you enter CLI successfully, the prompt display *Switch*> (the model name of your device together with a greater than sign) will appear on the screen.

Step 6. Set up the Smart Switch's IP address, subnet mask and the default gateway using "IP" command in Global Configuration mode. (See Section 2.5.5 IP command for detailed descriptions on assigning IP address to the Smart Switch.)

Step 7. Once you enter the new IP address for the Smart Switch, the telnet session will be terminated immediately. Use your new IP address to login to the Smart Switch via Telnet session.

Limitation: Only one active Telnet session can access the Smart Switch at a time.

2.2 Navigating CLI

When you successfully access the Smart Switch, you will be asked for a login username. Enter your authorized username and password, and then you will be directed to User mode. In CLI management, the User mode only provides users basic functions to operate the Smart Switch. If you would like to configure advanced features of the Smart Switch, such as, VLAN, QoS, you must enter the Configuration mode. The following table provides an overview of modes available in this Smart Switch.

Command Mode	Access Method	Prompt Displayed	Exit Method
User mode	Login username & password	`Switch>`	logout
Privileged mode	From user mode, enter the *enable* command	`Switch#`	disable, exit, logout
Configuration mode	From the enable mode, enter the *config* or *configure* command	`Switch(config)#`	exit

NOTE: *By default, the model name will be used for the prompt display. You can change the prompt display to the one that is ideal for your network environment using the hostname command. However, for convenience, the prompt display "Switch" will be used throughout this user's manual.*

2.2.1 General Commands

This section introduces you some general commands that you can use in User, Enable, and Configuration mode, including "help", "exit", "history" and "logout".

Entering the command…	To do this…	Available Modes

`Switch> help`
`Switch# help`
`Switch(config)# help`
	Obtain a list of available commands in the current mode.	User Mode
		Privileged Mode
		Configuration Mode

`Switch> exit`
`Switch# exit`
`Switch(config)# exit`
	Return to the previous mode or login screen.	User Mode
		Privileged Mode
		Configuration Mode

`Switch> history`
`Switch# history`
`Switch(config)# history`
	List all commands that have been used.	User Mode
		Privileged Mode
		Configuration Mode

`Switch> logout` `Switch# logut`	Logout from the CLI or terminate Telnet session.	User Mode Privileged Mode

2.2.2 Quick Keys

In CLI, there are several quick keys that you can use to perform several functions. The following table summarizes the most frequently used quick keys in CLI.

Keys	Purpose
tab	Enter an unfinished command and press “Tab” key to complete the command.
?	Press “?” key in each mode to get available commands.

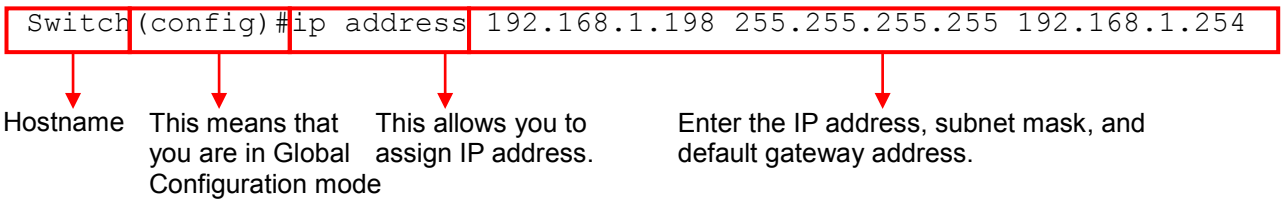
unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Example 1: List all available commands starting with the characters that you enter.
	
	`Switch#h?`
	`help  Show available commands`
	`history  Show history commands`
	
	`Switch#he?`
	`<cr>`
	
	`Switch#help`
	
	Example 2: Complete a valid command and show the next part of syntax.
	
	`Switch(config)#sec?`
	`storm-protection  Storm control subcommands`
	`Switch(config)#security`

Up arrow	Use Up arrow key to scroll through the previous entered commands, beginning with the most recent key-in commands.
Down arrow	Use Down arrow key to scroll through the previous entered commands, beginning with the commands that are entered first.

2.2.3 Command Format

While in CLI, you will see several symbols very often. As mentioned above, you might already know what “>”, “#” and (config)# represent. However, to perform what you intend the device to do, you have to enter a string of complete command correctly. For example, if you want to assign IP address for the Smart Switch, you need to enter the following command with the required parameter and IP, subnet mask and default gateway:

IP command syntax: `Switch(config)#ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]`


Switch(config)#ip address 192.168.1.198 255.255.255.255 192.168.1.254
Hostname
This means that you are in Global Configuration mode
This allows you to assign IP address.
Enter the IP address, subnet mask, and default gateway address.

The following table lists common symbols and syntax that you will see very frequently in this User's Manual for your reference:

Symbols	Brief Description
>	Currently, the device is in User mode.
#	Currently, the device is in Privileged mode.
(config)#	Currently, the device is in Global Configuration mode.

Syntax	Brief Description
[ ]	Brackets mean that this field is required information.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port-based | 802.1p | dscp]	There are three options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.

[0-7] 802.1p_list
[0-63] dscp_list
	Specify one value, more than one value or a range of values.
	
	For example: specifying one value
	
	`Switch(config)#qos 802.1p-map 1 0`
	
	`Switch(config)#qos dscp-map 10 3`
	
	For example: specifying three values (separating by a comma)
	
	`Switch(config)#qos 802.1p-map 1,3 0`
	
	`Switch(config)#qos dscp-map 10,13,15 3`
	
	For example: specifying a range of values (separating by a hyphen)
	
	`Switch(config)#qos 802.1p-map 1-3 0`
	
	`Switch(config)#qos dscp-map 10-15 3`

2.2.4 Login Username & Password

Default Login

When you enter Telnet session, a login prompt for username and password will appear to request a valid and authorized username and password combination. For first-time users, enter the default login username "**admin**" and "**press Enter key**" in password field (no password is required for default setting). When system prompt shows "Switch>", it means that the user has successfully entered the User mode.

For security reasons, it is strongly recommended that you add a new login username and password using User command in Configuration mode. When you create your own login username and password, you can delete the default username (admin) to prevent unauthorized access.

2.3 User Mode

In User mode, only a limited set of commands are provided. Please note that in Use mode, you have no authority to configure advanced settings. You need to enter Enable mode and Configuration mode to set up advanced functions of a switch feature. For a list of commands available in User mode, enter the question mark (?) or “help” command after the system prompt display Switch>.

Command	Description
exit	Quit the User mode or close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the Smart Switch.
enable	Enter the Privileged mode.
ping	Ping a remote host.

2.3.1 Ping command

Ping is used to test the connectivity of end devices and also can be used to self test the network interface card. Enter the **ping** command in User mode. In this command, you can add an optional packet size value and an optional value for the number of times that packets are sent and received.

Command	Parameter	Description
Switch> ping [A.B.C.D] [-s size] [-r repeat] [-t timeout]	[A.B.C.D]	Enter the IP address that you would like to ping.
	[-s size]	Enter the packet size that would be sent. The allowable packet size is from 8 to 4000 bytes. The parameter is optional.
	[-r repeat]	Enter the number of times that ping packets are sent. The allowable repeat number is from 1 to 99. The parameter is optional.
	[-t timeout]	Enter the timeout value when the specified IP address is not reachable. The parameter is optional.
Example		
Switch> ping 127.0.0.1		
Switch> ping 127.0.0.1 –s 128 –r 5 –t 10		

2.4 Privileged mode

The only place where you can enter the Privileged (Enable) mode is in User mode. When you successfully enter Enable mode, the prompt will be changed to Switch# (the model name of your device together with a pound sign). Enter the question mark (?) or help command to view a list of commands available for use.

Command	Description
copy-cfg	Restore or backup configuration file via FTP or TFTP server.
configure	Enter Global Configuration mode.
disable	Exit Enable mode and return to User Mode.
exit	Exit Enable mode and return to User Mode.
firmware	Upgrade firmware via FTP or TFTP.
help	Display a list of available commands in Enable mode.
history	Show commands that have been used.
logout	Logout from the Managed Switch.
reload	Restart the Managed Switch.
write	Save your configurations to Flash.
show	Show a list of commands or show the current setting of each listed command.
ping	Ping a remote host.

2.4.1 Copy-cfg command

Use “copy-cfg” command to backup a configuration file via FTP or TFTP server or restore the Smart Switch back to the defaults or to the defaults but keep IP configurations.

1. Restore a configuration file via FTP or TFTP server.

Command	Parameter	Description
Switch# copy-cfg from ftp [A.B.C.D] [file_name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the configuration file name that you want to restore.
	[user_name]	Enter the username for your FTP server.
	[password]	Enter the password for your FTP server.
Switch# copy-cfg from tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the configuration file name that you want to restore.
Example		
Switch# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misabcxyz 135780		
Switch# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

2. Restore the Smart Switch back to default settings.

Command / Example
Switch# copy-cfg from default

3. Restore the Smart Switch back to default settings but keep IP configurations.

Command / Example
Switch# copy-cfg from default keep-ip

4. Backup a configuration file to FTP or TFTP server.

Command	Parameter	Description
Switch# copy-cfg to ftp [A.B.C.D] [file_name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file_name]	Enter the configuration file name that you want to backup.
	[user_name]	Enter the username for your FTP server.
	[password]	Enter the password for your FTP server.
Switch# copy-cfg to tftp [A.B.C.D] [file name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file name]	Enter the configuration file name that you want to backup.
Example		
Switch# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf misabcxyz 135780		
Switch# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf		

2.4.2 Firmware command

To upgrade Firmware via FTP or TFTP server.

Command	Parameter	Description
Switch# firmware upgrade ftp [A.B.C.D] [file_name] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file name]	Enter the firmware file name that you want to upgrade.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Switch# firmware upgrade tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the firmware file name that you want to upgrade.
Example		
Switch# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin edgeswitch10 abcxyz		
Switch# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin		

2.4.3 Ping command

Command	Parameter	Description
Switch# ping [A.B.C.D] [-s size] [-r repeat] [-t timeout]	[A.B.C.D]	Enter the IP address that you would like to ping.
	[-s size]	Enter the packet size that would be sent. The allowable packet size is from 8 to 4000 bytes. The parameter is optional.
	[-r repeat]	Enter the number of times that ping packets are sent. The allowable repeat number is from 1 to 99. The parameter is optional.
	[-t timeout]	Enter the timeout value when the specified IP address is not reachable. The parameter is optional.
Example		
Switch# ping 127.0.0.1 –s 128 –r 5 –t 10		

2.4.4 Reload command

To restart the Smart Switch, enter the reload command.

Command / Example
Switch# reload

2.4.5 Write command

To save running configurations to startup configurations, enter the write command. All unsaved configurations will be lost when you restart the Smart Switch.

Command / Example
Switch# write

2.4.6 Configure command

The only place where you can enter Global Configuration mode is in Privileged mode. You can type in “configure” or “config” for short to enter Global Configuration mode. The display prompt will change from “Switch#” to “Switch(config)#” once you successfully enter Global Configuration mode.

Command / Example
Switch#config Switch(config)#
Switch#configure Switch(config)#

2.5 Configuration mode

When you enter “configure” or “config” and press “Enter” in Privileged mode, you will be directed to Global Configuration mode where you can set up advanced switching functions, such as QoS, VLAN and storm control security globally. Any commands entered will apply to running-configuration and the device’s operation. From this level, you can also enter different sub-configuration modes to set up specific configurations for VLAN, QoS, security or interfaces.

Command	Description
exit	Exit the configuration mode.
help	Display a list of available commands in Configuration mode.
history	Show commands that have been used.
ip	Set up the IP address and enable DHCP mode & IGMP snooping.
mac	Set up each port’s MAC learning function.
qos	Set up the priority of packets, DSCP mapping.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
switch-info	Set up acceptable frame size and address learning, etc.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or set it back to its default setting.
interface	Select a single interface or a range of interfaces.
show	Show a list of commands or show the current setting of each listed command.

2.5.1 Entering Interface Numbers

In the Global Configuration mode, you can configure a command that only apply to interfaces specified. For example, you can set up each interface’s VLAN assignment, speeds, or duplex modes. To configure, you must first enter the interface number. There are four ways to enter your interface numbers to signify the combination of different interfaces that apply to a command or commands.

Commands	Description
Switch(config)# interface 1 Switch(config-if)#	Enter a single interface. Only interface 1 will apply to commands entered.
Switch(config)# interface 1,3 Switch(config-if)#	Enter three discontinuous interfaces, separating by a comma. Interface 1, 3 will apply to commands entered.
Switch(config)#interface 1-3 Switch(config-if)#	Enter three continuous interfaces. Use a hyphen to signify a range of interface numbers. In this example, interface 1, 2, and 3 will apply to commands entered.
Switch(config)#interface 1,3-4 Switch(config-if)#	Enter a single interface number together with a range of interface numbers. Use both comma and hyphen to signify the combination of different interface numbers. In this example, interface 1, 3, 4 will apply to commands entered.

The “interface” command can be used together with “QoS” and “VLAN” commands. For detailed usages, please refer to QoS and VLAN section below.

2.5.2 No command

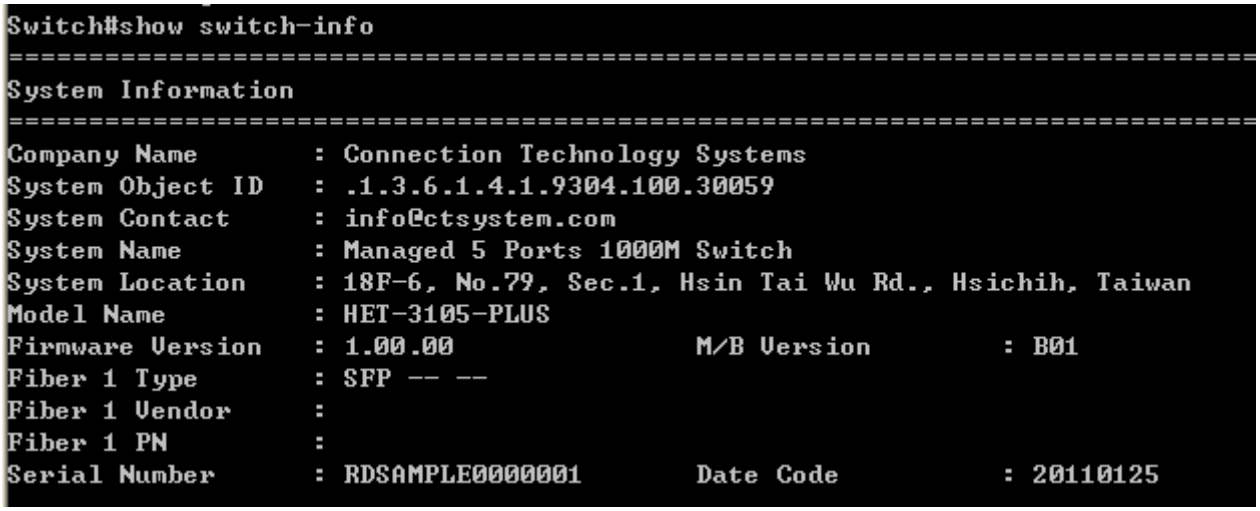
Almost commands that you enter in Configuration mode can be negated using “no” command followed by the same or original command. The purpose of “no” command is to disable a function, remove a command, or set the setting back to the default value. In each sub-section below, the use of no command to fulfill different purposes will be introduced.

2.5.3 Show command

“show” command is very important for network administrators to get information about the device, receive outputs to verify a command’s configurations or troubleshoot a network configuration error. “Show” command can be either used in Privileged or Configuration mode. The following describes different uses of “show” command.

1. Display system information

Enter “show switch-info” command in Privileged or Configuration mode, then the following similar screen page will appear.


Switch#show switch-info
System Information
Company Name : Connection Technology Systems
System Object ID : .1.3.6.1.4.1.9304.100.30059
System Contact : info@ctsystem.com
System Name : Managed 5 Ports 1000M Switch
System Location : 18F-6, No.79, Sec.1, Hsin Tai Wu Rd., Hsichih, Taiwan
Model Name : HET-3105-PLUS
Firmware Version : 1.00.00 M/B Version : B01
Fiber 1 Type : SFP -- --
Fiber 1 Vendor :
Fiber 1 PN :
Serial Number : RDSAMPLE0000001 Date Code : 20110125

Company Name: Display a company name for this Smart Switch. Use “switch-info company-name [company-name]” command to edit this field.

System Object ID: Display the predefined System OID.

System Contact: Display contact information for this Smart switch. Use “switch-info sys-contact [sys-contact]” command to edit this field.

System Name: Display a descriptive system name for this Smart Switch. Use “switch-info sys-name [sys-name]” command to edit this field.

System Location: Display a brief location description for this Smart Switch. Use “switch-info sys-location [sys-location]” command to edit this field.

Model Name: Display the product’s model name.

Firmware Version: Display the firmware version used in this device.

M/B Version: Display the main board version.

Fiber Type: Display information about the slide-in or fixed fiber type.

Fiber Wavelength: Display the slide-in or fixed fiber’s TX and RX wavelength information.

Serial Number: Display the serial number of this Smart Switch.

Date Code: Display the Smart Switch Firmware date code.

2. Display or verify currently-configured settings

Refer to “Interface command”, “QoS command” and “VLAN command” sections.

2.5.4 Interface command

Use this command to set up various port configurations of discontinuous or a range of ports.

Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several port numbers separating by a comma or a range of port numbers. For example: 1,3 or 2-4
Switch(config-if)# speed [1000 | 100 |10 | auto-sense]	[1000 | 100 |10 | auto-sense]	Set up the selected interfaces' speed. "auto-sense" option is used for fiber port only. This option allows the Smart Switch to automatically detect fiber speed of the connected device.
Switch(config-if)# auto-negotiation		Set the selected interfaces' to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored.
Switch(config-if)# duplex [full]	[full]	Set the selected interfaces' to full duplex mode.
Switch(config-if)# flowcontrol		Enable the selected interfaces' flow control function.
Switch(config-if)# shutdown		Administratively disable the selected ports' status.
No command		
Switch(config-if)# no auto-negotiation		Set auto-negotiation setting to the default setting.
Switch(config-if)# no duplex		Set the selected ports' duplex mode to the default setting.
Switch(config-if)# no flowcontrol		Set the selected ports' flow control function to the default setting.
Switch(config-if)# no shutdown		Administratively enable the selected ports' status.
Switch(config-if)# no speed		Set the selected ports' speed to the default setting.
Show command		
Switch(config)# show interface		Show each interface's port configurations.
Switch(config)# show interface [port_list]	[port_list]	Show the specified interfaces' port configurations.
Switch(config)# show interface status		Show each interface's port status including media type, forwarding state, speed, duplex mode, flow control and link up/down status.
Switch(config)# show interface status [port_list]	[port_list]	Show the specified interface's port status including media type, forwarding state, speed, duplex mode, flow control and link up/down status.

Interface command example	
Switch(config)# interface 1-3	Enter port 1 to port 3's interface mode.
Switch(config-if)# auto-negotiation	Set the selected interfaces' to auto-negotiation.
Switch(config-if)# duplex full	Set the selected interfaces' to full duplex mode.
Switch(config-if)# flowcontrol	Enable the selected interfaces' flow control function.
Switch(config-if)# speed 100	Set the selected ports' speed to 100Mbps.
Switch(config-if)# shutdown	Administratively disable the selected ports' status.

2.5.5 IP command

1. Set up or remove the IP address of the Smart Switch.

IP command	Parameter	Description
Switch(config)#ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]	[A.B.C.D]	Enter the desired IP address for your Smart Switch.
	[255.X.X.X]	Enter subnet mask of your IP address.
	[A.B.C.D]	Enter the default gateway address.
No command		
Switch(config)# no ip address		Remove the Smart Switch's IP address.
Show command		
Switch(config)# show ip address		Show the current IP configurations or verify the configured IP settings.
IP command example		
Switch(config)# ip address 192.168.1.198 255.255.255.0 192.168.1.254		Set up the Smart Switch's IP to 192.168.1.198, subnet mask to 255.255.255.0, and default gateway to 192.168.1.254.

2. Enable the Smart Switch to automatically get IP address from the DHCP server.

Command / Example	Description
Switch(config)# ip address dhcp	Enable DHCP mode.
No command	
Switch(config)# no ip address dhcp	Disable DHCP mode.
Show command	
Switch(config)# show ip address	Show the current IP configurations or verify the configured IP settings.

3. Enable or disable IGMP snooping globally.

IGMP, Internet Group Management Protocol, is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used for online streaming video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 packets IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. A switch using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces the workload at the end hosts since their network cards (or operating system) will not have to receive and filter all the multicast traffic generated in the network.

Command / Example	**Description**
Switch(config)# ip igmp snooping	Enable IGMP snooping function.
No command	
Switch(config)# no ip igmp snooping	Disable IGMP snooping function.
Show command	
Switch(config)# show ip igmp snooping	Show current IGMP snooping status including fast leave function.
Switch(config)#show ip igmp snooping groups	Show IGMP group table. When IGMP Snooping is enabled, the Smart Switch is able to read multicast group IP and the corresponding MAC address from IGMP packets that enter the device.

4. Enable IGMP snooping fast-leave function. This works only when IGMP Snooping is enabled. When Fast Leave is enabled, the Smart Switch immediately removes the port when it detects IGMPv1 & IGMPv2 leave message on that port.

Command / Example	Description
Switch(config)# ip igmp snooping immediate-leave	Enable IGMP fast leave function.
No command	**Description**
Switch(config)# no ip igmp snooping immediate-leave	Disable IGMP fast leave function.
Show command	**Description**
Switch(config)# show ip igmp snooping	Show current IGMP snooping status including fast leave function.
Switch(config)# show ip igmp snooping groups	Show IGMP group table.

2.5.6 MAC command

Set up MAC address table aging time. Entries in the MAC address table containing source MAC addresses and their associated ports will be deleted if they are not accessed within aging time.

MAC Command	Parameter	Description
Switch(config)# mac address-table aging-time [0-458745]	[0-458745]	Enter the aging time for MAC addresses in seconds.
No command		**Description**
Switch(config)# no mac address-table aging-time		Set MAC address table aging time to the default value (300 seconds).
Show command		**Description**
Switch(config)# show mac aging-time		Show current MAC address table aging time or verify currently configured aging time.
MAC command example		**Description**
Switch(config)# mac address-table aging-time 200		Set MAC address aging time to 200 seconds.

2.5.7 QoS command

1. Specify the desired QoS mode.

QoS command	Parameter	Description
Switch(config)#qos [port-based | 802.1p | dscp]	[port-based | 802.1p | dscp]	Specify one QoS mode. **port-based:** Use "*interface"* and "*qos default-class"* command to assign a queue to the selected interfaces. **802.1p:** Use *"802.1p-map [0-7] 802.1p_list [0-3]"* command to assign priority bits to a queue. **dscp:** Use "*dscp-map [0-63] dscp_list [0-3]"* to assign several DSCP values to a queue.
No command		**Description**
Switch(config)# no qos		Disable QoS function.
Show command		**Description**
Switch(config)# show qos		Show or verify QoS configurations.
QoS command example		
Switch(config)# qos 802.1p		Enable QoS function and use 802.1p mode.
Switch(config)# qos dscp		Enable QoS function and use DSCP mode.
Switch(config)# qos port-based		Enable QoS function and use Port-Based mode.

2. Set up the DSCP and queue mapping.

DSCP-map command	Parameter	Description
Switch(config)# qos dscp-map [0-63] dscp_list [0-3]	[0-63] dscp_list	Specify the corresponding DSCP value or values that you want to map to a priority queue value.
	[0-3]	Set up the corresponding queue.
No command		
Switch(config)# no qos		Disable QoS function
Show command		
Switch(config)# show qos		Show or verify QoS configurations.

DSCP-map example	
Switch(config)# qos dscp-map 10-50 3	Mapping DSCP values from 10 to 50 to queue 3.

3. Set up QoS queuing mode.

Queuing-mode command	Parameter	Description
Switch(config)# qos queuing-mode [weight]	[weight]	By default, “weight” queuing mode is used. If you want to use “strict” queuing mode, you need to disable “weight” queuing mode. **Weight mode**: This mode enables users to assign different weights (0 to 49) to 4 queues. **Strict mode:** This indicates that services to each egress queues are offered depending on the maximum rate (1000Mbps).
No command		
Switch(config)# no qos queuing-mode		Set the queuing mode to Strict mode.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
Queuing-mode example		
Switch(config)# qos queuing-mode weight		Change the queuing mode from strict to weight.

4. Set up queuing weight.

Queue-weighted command	Parameter	Description
Switch(config)# qos queue-weighted [1:2:4:8]	[1:2:4:8]	By default, schedule weight for Q0, Q1, Q2, Q3 is “1:1:1:1”. Use *“qos queue-weighted 1:2:4:8”* to change each queue’s weight to the corresponding one. The weight value can be assigned to each queue is between 0 and 49.
No command		
Switch(config)# no qos queue-weighted		Change queue weight to 1:1:1:1.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.

Queuing-mode example	
Switch(config)# qos queue-weighted 1:2:4:8	Change queue weight to 1:2:4:8.

5. Assign a tag priority to the specific queue.

802.1p-map command	Parameter	Description
Switch(config)# qos 802.1p-map [0-7] 802.1p_list [0-3]	[0-7] 802.1p_list	Assign a 802.1p priority bit or several 802.1p priority bits for mapping.
	[0-3]	Assign a 802.1p queue value for mapping.
No command		
Switch(config)# no qos 802.1p-map [0-7] 802.1p_list	[0-7] 802.1p_list	Assign a 802.1p priority bit or several 802.1p priority bits that you want to delete or remove.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
802.1p-map example		
Switch(config)# qos 802.1p-map 6-7 3		Map priority bit 6 and 7 to queue 3.

6. Use interface command to set up default class for the selected interfaces.

QoS & Interface command	Parameter	Description
Switch(config-if)# qos default-class [0-3]	[0-3]	Specify the selected interfaces' default queue.
No command		**Description**
Switch(config-if)# no qos default-class		Set QoS default class setting back to defaults.
Show command		**Description**
Switch(config)#show qos		Show or verify QoS configurations.
QoS & Interface example		**Description**
Switch(config)# interface 1-3		Enter several discontinuous port numbers separating by a comma or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if)# qos default-class 3		Set the selected ports' default class to 3.

2.5.8 SNMP-Server command

1. Create a SNMP community and set up detailed configurations for this community.

Snmp-server command	Parameter	Description
Switch(config)# snmp-server community [community]	[community]	Specify a SNMP community name of up to 20 alphanumeric characters.
Switch(config-snmp-server)# active		Enable this SNMP community account.
Switch(config-snmp-server)# description [Description]	[Description]	Enter the description for this SNMP community of up to 35 alphanumerical characters.
Switch(config-snmp-server)#level [admin | rw | ro | access_denied]	[admin | rw | ro | access_denied]	Specify the access privilege for this SNMP account. **admin:** Full access right includes maintaining user account, system information, loading factory settings, etc. **rw:** Read & Write access privilege. Full access right but cannot modify user account, system information and load factory settings. **ro:** Read Only access privilege. Allow to view only. **access_denied:** Completely forbidden for access.
No command		
Switch(config)# no snmp-server community mycomm		Delete the community “mycomm”.
Switch(config-snmp-server)# no active		Disable this SNMP community account. In this example “mycomm” community is disabled.
Switch(config-snmp-server)# no description		Remove the entered SNMP community descriptions for “mycomm”.
Switch(config-snmp-server)# no level		Remove the configured level. This will set this community’s level to access_denied.
Show command		
Switch(config)# show snmp-server community mycomm		Show SNMP community account’s information in Global Configuration mode.
Switch(config-snmp-server)# show		View or verify the configured SNMP community account’s information.

Exit command	
Switch(config-snmp-server)#exit	Return to Global Configuration mode.
Snmp-server example	
Switch(config)# snmp-server community mycomm	Create a new community “mycomm” and edit the details of this community account.
Switch(config-snmp-server)# active	Activate the SNMP community “mycomm”.
Switch(config-snmp-server)# description rddeptcomm	Add a description for “mycomm” community.
Switch(config-snmp-server)# level admin	Set “mycomm” community level to admin.

2. Set up a SNMP trap destination.

Trap-dest command	Parameter	Description
Switch(config)#snmp-server trap-destination [1]	[1]	Create a trap destination account.
Switch(config-snmp-server)# active		Enable this SNMP trap destination account.
Switch(config-snmp-server)# community [community]	[community]	Enter the community name of network management system.
Switch(config-snmp-server)# destination [A.B.C.D]	[A.B.C.D]	Enter the trap destination IP address for this trap destination account.
No command		**Description**
Switch(config)# no snmp-server trap-dest 1		Delete a trap destination account.
Switch(config-snmp-server)# no active		Disable this SNMP trap destination account.
Switch(config-snmp-server)# no community		Delete the configured community name.
Switch(config-snmp-server)# no description		Delete the configured trap destination description.
Show command		**Description**
Switch(config)# show snmp-server trap-dest		Show SNMP trap destination information.
Switch(config)# show snmp-server trap-dest 1		Show the specified SNMP trap destination information.
Exit command		**Description**
Switch(config-snmp-server)# exit		Return to Global Configuration mode.
Trap-dest example		**Description**
Switch(config)# snmp-server trap-dest 1		Create a trap destination account.

Switch(config-snmp-server)# active	Activate the trap destination account.
Switch(config-snmp-server)# community mycomm	Refer this trap destination account to the community “mycomm”.
Switch(config-snmp-server)# description redepttrapdest	Add a description for this trap destination account.
Switch(config-snmp-server)# destination 192.168.1.254	Set trap destination IP address to 192.168.1.254.

3. Set up SNMP trap types that will be sent.

Trap-type command	**Parameter**	**Description**
Switch(config)# snmp-server trap-type [all |auth-fail | cold-start | port-link | power-down | warm-start]	[all |auth-fail | cold-start | port-link | power-down | warm-start]	Specify the trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, the device cold /warm starts, port link is up or down and power is down. **auth-fail:** A trap will be sent when any unauthorized users attempt to login. **cold-start:** A trap will be sent when the device boots up. **port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the device’s power is down. **warm-start:** A trap will be sent when the device restarts.
No command		**Description**
Switch(config)# no snmp-server trap-type auth-fail	all |auth-fail | cold-start | port-link | power-down | warm-start]	Specify the trap type that will not be sent.
Show command		**Description**
Switch(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Trap-type example		**Description**
Switch(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

2.5.9 Switch-info command

Set up the Smart Switch's basic information including company name, hostname, system name, etc.

Switch-info Command	Parameter	Description
Switch(config)# switch-info company-name [company-name]	[company-name]	Enter a company name for this Smart Switch, up to 55 alphanumeric characters.
Switch(config)# switch-info host-name [host-name]	[host-name]	Change the model name for this Managed Switch, up to 15 alphanumeric characters.
Switch(config)# switch-info system-contact [sys-contact]	[sys-contact]	Enter contact information for this Managed switch, up to 55 alphanumeric characters.
Switch(config)# switch-info system-location [sys-location]	[sys-location]	Enter a brief description of the Managed Switch location, up to 55 alphanumeric characters. Like the name, the location is for reference only, for example, "13th Floor".
Switch(config)# switch-info system-name [sys-name]	[sys-name]	Enter a unique name for this Managed Switch, up to 55 alphanumeric characters. Use a descriptive name to identify the Managed Switch in relation to your network, for example, "Backbone 1". This name is mainly used for reference only.
No command		
Switch(config)# no switch-info company-name		Delete the entered company name information.
Switch(config)# no switch-info host-name		Delete the entered switch model name information.
Switch(config)# no switch-info system-contact		Delete the entered system contact information.
Switch(config)# no switch-info system-location		Delete the entered system location information.
Switch(config)# no switch-info system-name		Delete the entered system name information.
Show command		
Switch(config)# show switch-info		Show switch information including company name, system contact, system location, system name, model name, firmware version and fiber type.
Switch-info example		
Switch(config)# switch-info company-name telecomxyz		Set the company name to "telecomxyz".
Switch(config)# switch-info host-name		Set the switch model name to "model 1"

model 1	
Switch(config)# switch-info system-contact info@company.com	Set the system contact field to “info@compnay.com”.
Switch(config)# switch-info system-location 13thfloor	Set the system location field to “13thfloor”.
Switch(config)# switch-info system-name backbone1	Set the system name field to “backbone1”.

2.5.10 User command

Create a new login account.

User command	Parameter	Description
Switch(config)# user name [user_name]	[user_name]	Enter the new account’s username. The authorized user login name is up to 20 alphanumeric characters. Only 3 login accounts can be registered in this device.
Switch(config-user)# description [description]	[description]	Enter the brief description for this user account.
Switch(config-user)# password [password]	[password]	Enter the password for this user account of up to 20 alphanumeric characters.
No command		
Switch(config)# no user name [user_name]	[user_name]	Delete the specified account.
Switch(config-user)# no description		Remove the configured description.
Switch(config-user)# no password		Remove the configured password value.
Show command		
Switch(config)# show user name		List all user accounts.
Switch(config)# show user name [user_name]	[user_name]	Show the specified account’s information.
Switch(config-user)# show		Show or verify the newly-created user account’s information.
User command example		
Switch(config)# user name miseric		Create a new login account “miseric”.
Switch(config-user)# level admin		Set “miseric” user level to admin.
Switch(config-user)# description misengineer		Add a description to this new account “miseric”.
Switch(config-user)# password mis2256i		Set up a password for this new account “miseric”

2.5.11 VLAN command

Create a 802.1q VLAN, management VLAN and Port-Based VLAN rule.

VLAN dot1q command	Parameter	Description
Switch(config)# vlan dot1q-vlan		Globally enable 802.1q VLAN.
Switch(config)# vlan dot1q-vlan [1-4094]	[1-4094]	Enter a VID number to create a 802.1q VLAN.
Switch(config)# vlan management-vlan [1-4094] management-port [port_list]	[1-4094]	Enter the management VLAN ID.
	[port_list]	Specify the management port number.
VLAN & Interface command		
Switch(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separating by a comma or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
Switch(config-if)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).
Switch(config-if)# vlan dot1q-vlan mode trunk native		Enable native VLAN for untagged traffic.
Switch(config-if)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Set up the selected ports' PVID.
Switch(config-if)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Group the selected ports to a specified VLAN.
Switch(config-if)# vlan port-based [name]	[name] The names can be entered are: **port1vlan**, **port2vlan**, **port3vlan**, **port4vlan**, **port5vlan**	Set the selected ports to a specified port-based VLAN. By default, every port is a member port in each port-based VLAN.
No command		**Description**
Switch(config)# no vlan dot1q-vlan		Disable 802.1q VLAN globally.
Switch(config)# no vlan dot1q-vlan [1-4094]	[1-4094]	Delete the VID 100.
Switch(config)# no vlan port-based [name]	[name]	Remove or delete the selected port from the specified port-based VLAN.

Switch(config-if)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
Switch(config-if)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
Switch(config-if)#no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
Switch(config-if)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' VLAN 100 port membership. The selected ports are no longer member ports in VLAN 100.
Switch(config-if)# no vlan port-based [name]	[name]	Remove or delete the selected port from the specified port-based VLAN.
Show command		**Description**
Switch(config)# show vlan		Display global VLAN information including 802.1q VLAN Enable/Disable status and CPU VLAN ID.
Switch(config)# show vlan dot1q-vlan		Show 802.1q VLAN table.
Switch(config)# show vlan port-based		Show port-based VLAN table.
Switch(config)# show vlan interface		Show each interface's VLAN assignment and tagging information.
Switch(config)# show vlan interface [port_list]	[port_list]	Show the selected ports' VLAN assignment and tagging information.
VLAN dot1q & interface example		
Switch(config)# vlan dot1q-vlan		Enable 802.1q VLAN globally.
Switch(config)# vlan dot1q-vlan 100		Create a new VLAN 100.
Switch(config)# vlan management-vlan 1 management-port 1-3		Set port 1~3 to management ports.
Switch(config)# interface 1-3		Enter port 1 to port3's interface mode.
Switch(config-if)# vlan dot1q-vlan mode access		Set the selected ports to untagged.
Switch(config-if)#vlan dot1q-vlan mode trunk		Set the selected ports to tagged.
Switch(config-if)#vlan dot1q-vlan access-vlan 100		Set the selected ports' PVID to 100.
Switch(config-if)# vlan dot1q-vlan trunk-vlan 50		Group the selected ports to VLAN 50.
Switch(config-if)# vlan port-based port3vlan		Set the selected ports to "port3vlan" port-based VLAN group.

2.5.12 Show sfp command

When you slide-in SFP transceiver, detailed information about this module can be viewed by issuing this command.

Command	Description
Switch(config)#show sfp information	Display SFP information including transmission speed, distance, vendor's name, vendor's P/N and Vendor's S/N
Switch(config)#show sfp state	Display SFP information including temperature, voltage, TX Bias, TX power, RX power.

APPENDIX A: Set Up DHCP Auto-Provisioning

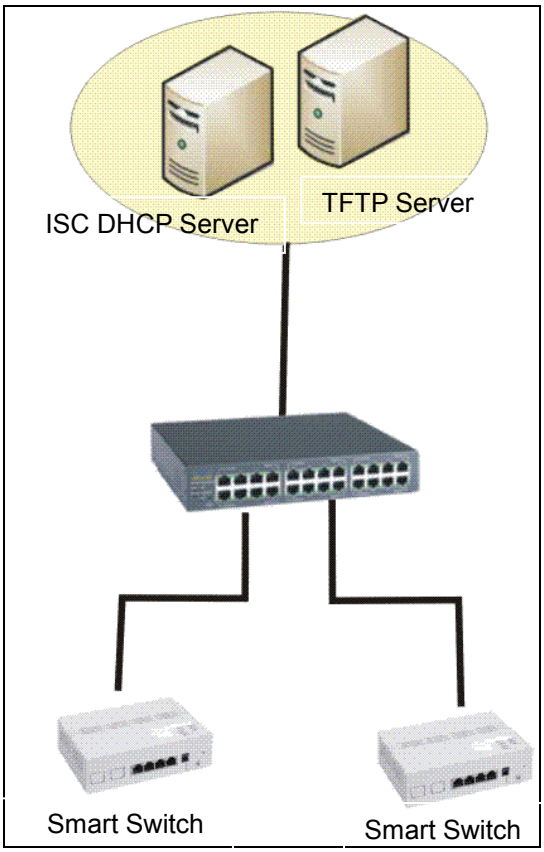
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased can support DHCP Auto-provisioning. Setup procedures and auto-provisioning process are described below for your reference.

A. Setup Procedures

Follow the steps below to set up Auto Provisioning server, modify dhcpd.conf file and generate a copy of configuration file.

Step 1. Setup Environment

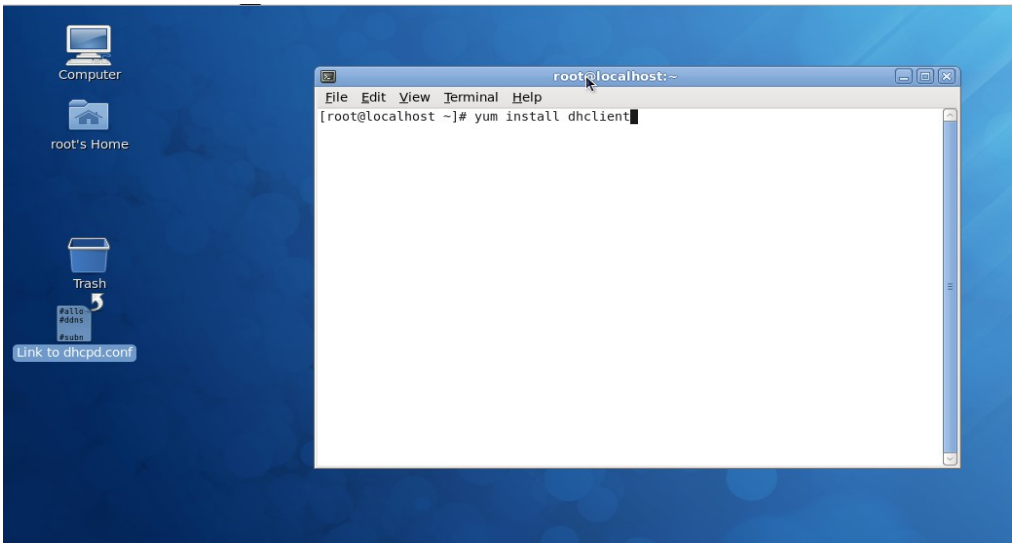
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Typology Example

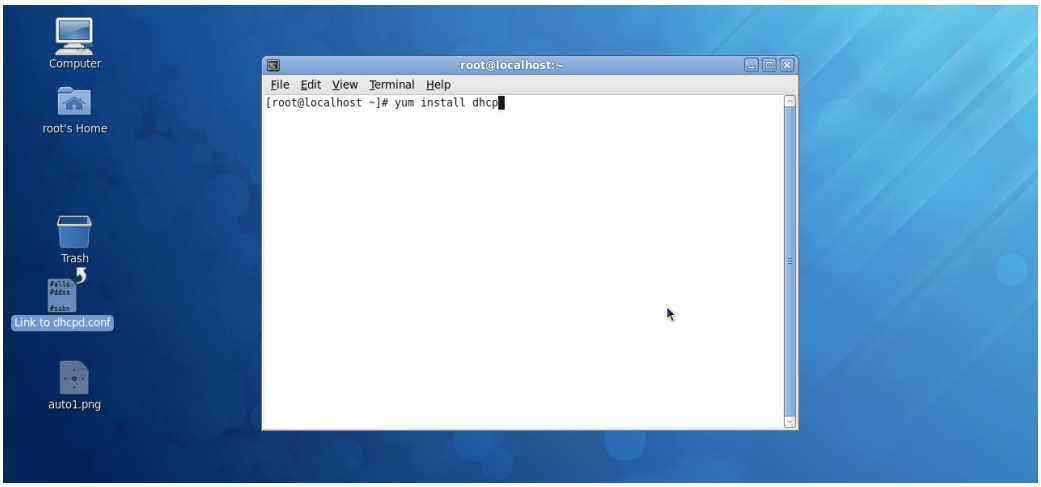
Step 2. Set up Auto Provision Server

- **Update DHCP Client**



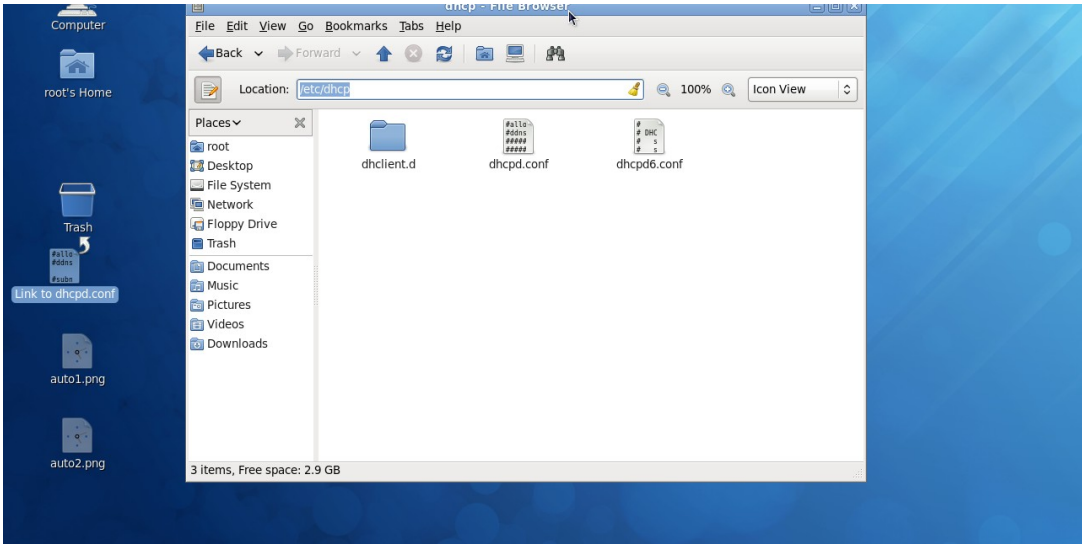
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP Server**



Issue “yum install dhcp” command to install DHCP server.

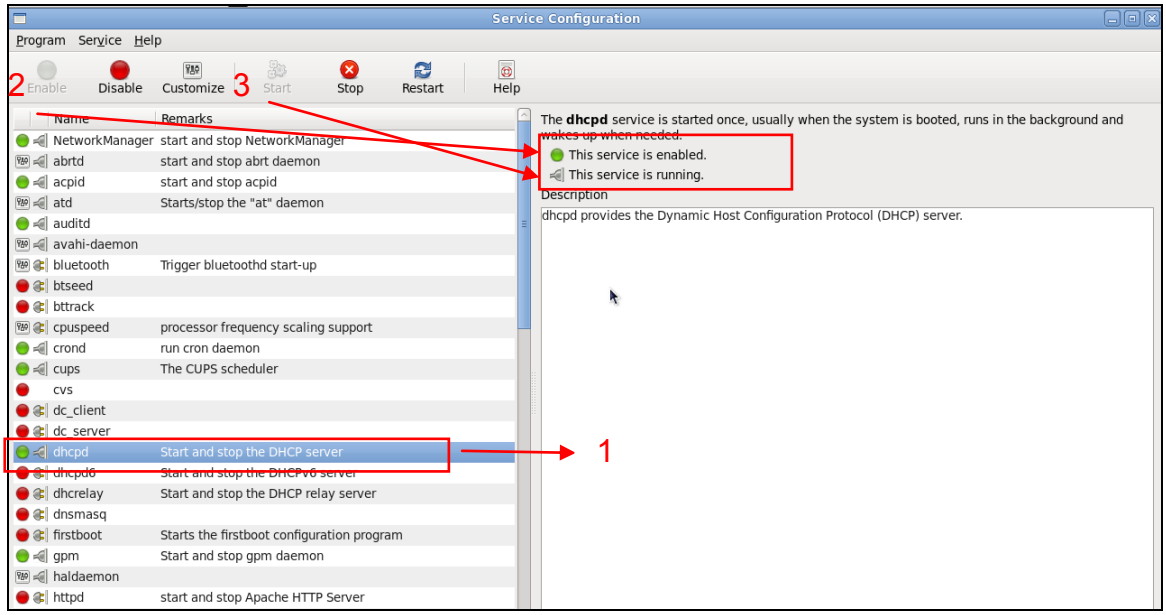
- **Copy dhcpd.conf to /etc/dhcp/ directory**



Copy dhcpd.conf file provided by the vendor to /etc/dhcp/ directory.

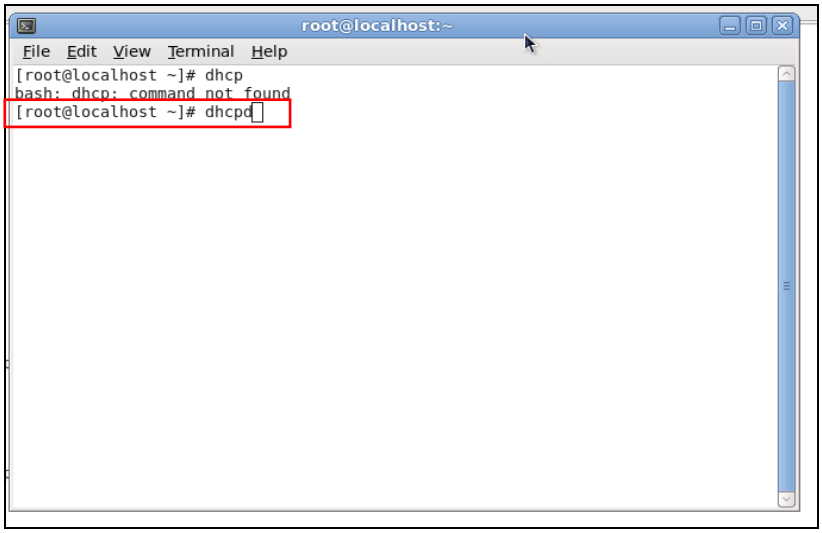
Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



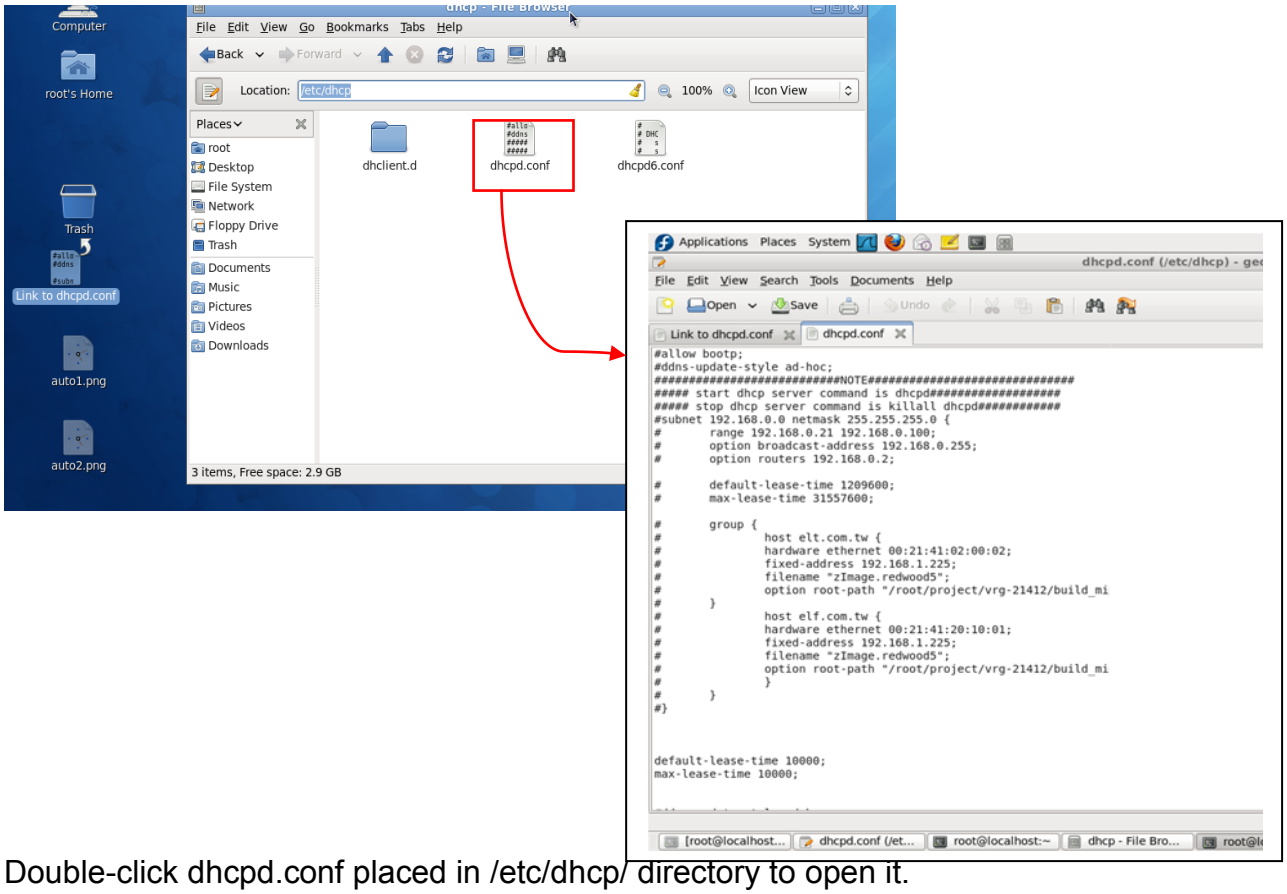
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

NOTE: *DHCP service can also be enabled using CLI. Issue "dhcpd" command to enable DHCP service.*



Step 3. Modify dhcpd.conf file

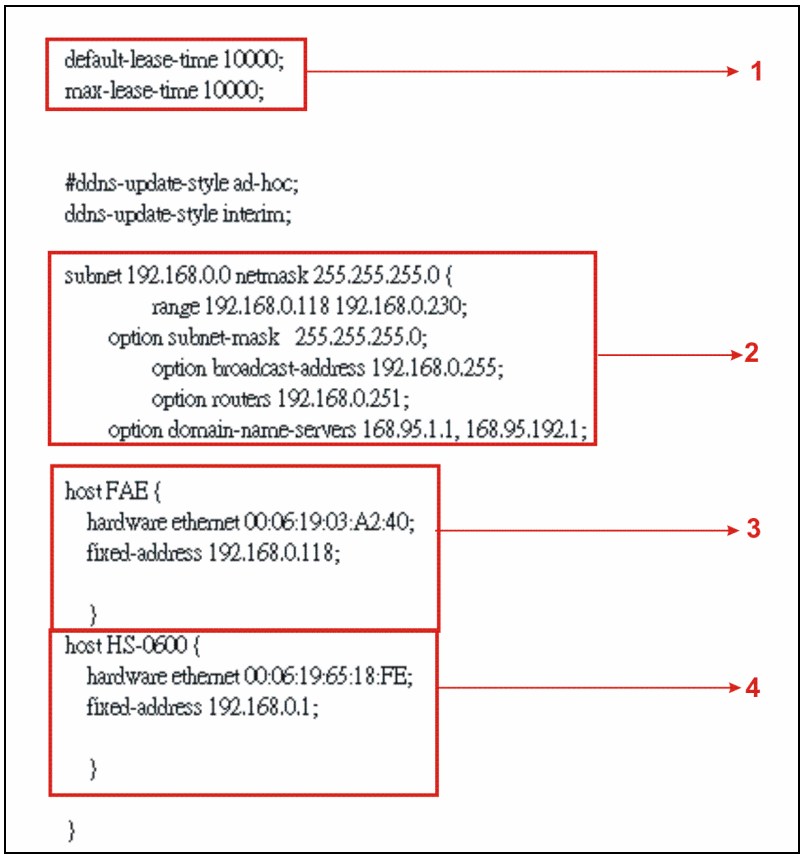
- **Open dhcpd.conf file in /etc/dhcp/ directory**



Double-click dhcpd.conf placed in /etc/dhcp/ directory to open it.

- **Modify dhcpd.conf file**

The following marked areas in dhcpd.conf file can be modified with values that work with your networking environment.



1. Define DHCP default and maximum lease time in seconds.

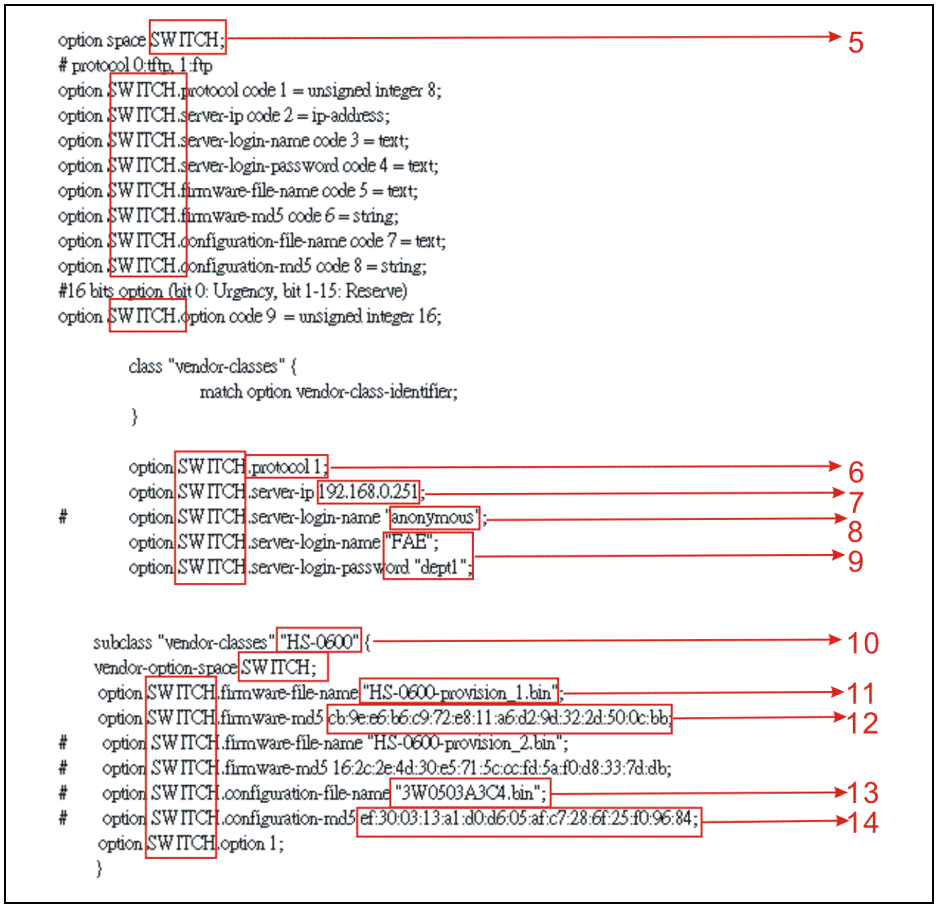
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   Maximum lease time: This is the maximum length of time that the server will lease for.

2. Define subnet, subnet mask, IP range, broadcast address, router address and DNS server address.

3. Map a host's MAC address to a fixed IP address.

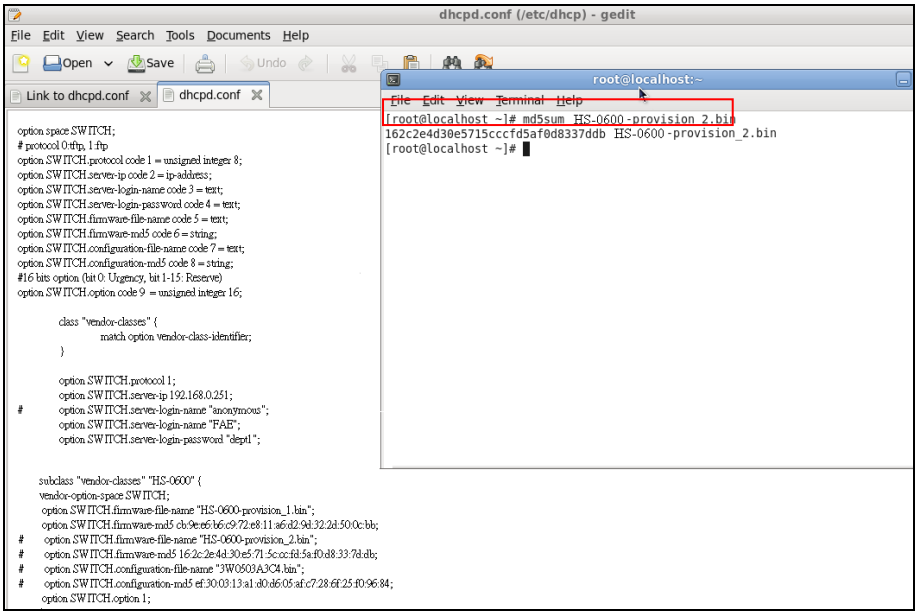
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



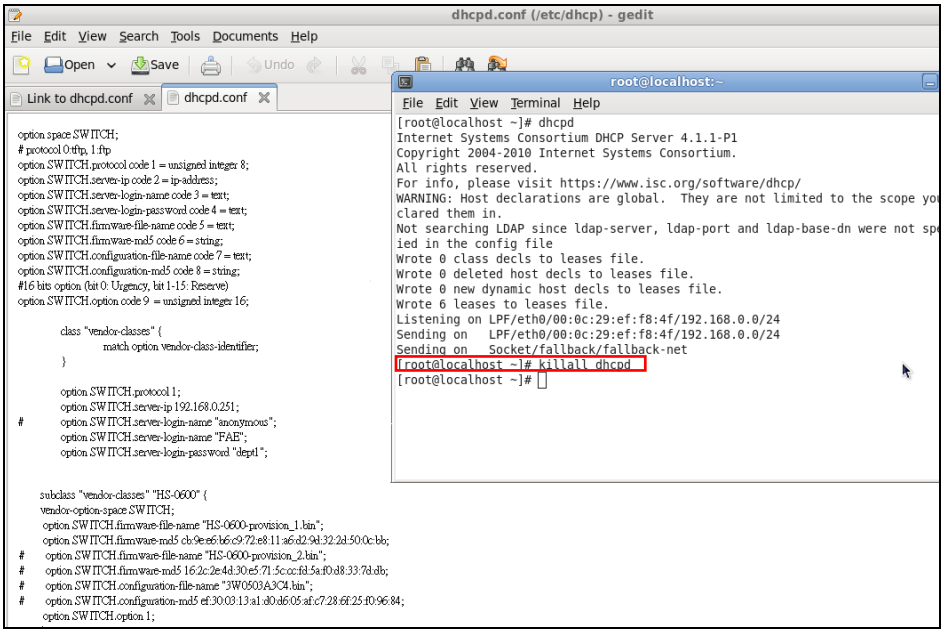
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify the product model name.
11. Specify the firmware filename.
12. Specify the MD5 for firmware image.
13. Specify the configuration filename.
14. Specify the MD5 for configuration file.

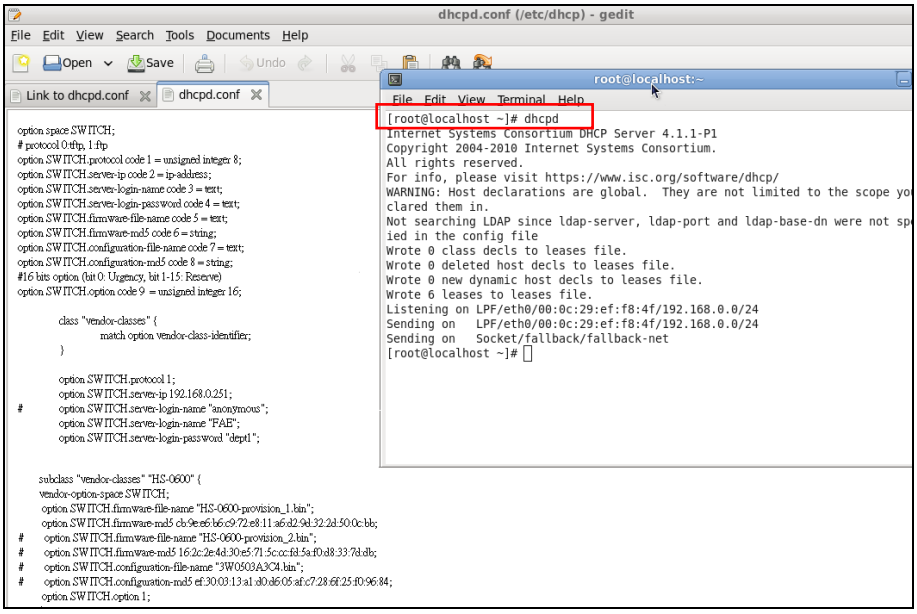
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs in the initial of each line.*

NOTE 2: *You can use either free software program or Linux default md5sum function to get MD5 checksum for firmware image and configuration file.*


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help
[root@localhost ~]# md5sum HS-0600-provision_2.bin
162c2e4d30e5715cccfd5af0d8337ddb HS-0600-provision_2.bin
[root@localhost ~]#
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9 = unsigned integer 16;
class "vendor-classes" {
match option vendor-class-identifier;
}
option SWITCH.protocol 1;
option SWITCH.server-ip 192.168.0.251;
option SWITCH.server-login-name "anonymous";
option SWITCH.server-login-name "FAE";
option SWITCH.server-login-password "dept1";
subclass "vendor-classes" "HS-0600" {
vendor-option-space SWITCH;
option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
option SWITCH.configuration-file-name "3W0503A3C4.bin";
option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
option SWITCH.option 1;

- **Restart DHCP service**


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help
[root@localhost ~]# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global. They are not limited to the scope yo
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not sp
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on Socket/fallback/fallback-net
[root@localhost ~]# killall dhcpd
[root@localhost ~]#
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9 = unsigned integer 16;
class "vendor-classes" {
match option vendor-class-identifier;
}
option SWITCH.protocol 1;
option SWITCH.server-ip 192.168.0.251;
option SWITCH.server-login-name "anonymous";
option SWITCH.server-login-name "FAE";
option SWITCH.server-login-password "dept1";
subclass "vendor-classes" "HS-0600" {
vendor-option-space SWITCH;
option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
option SWITCH.configuration-file-name "3W0503A3C4.bin";
option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
option SWITCH.option 1;


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help
[root@localhost ~]# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global. They are not limited to the scope yo
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not sp
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on Socket/fallback/fallback-net
[root@localhost ~]#
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9 = unsigned integer 16;
class "vendor-classes" {
match option vendor-class-identifier;
}
option SWITCH.protocol 1;
option SWITCH.server-ip 192.168.0.251;
option SWITCH.server-login-name "anonymous";
option SWITCH.server-login-name "FAE";
option SWITCH.server-login-password "dept1";
subclass "vendor-classes" "HS-0600" {
vendor-option-space SWITCH;
option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
option SWITCH.configuration-file-name "3W0503A3C4.bin";
option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
option SWITCH.option 1;

Every time when you modify dhcpd.conf file, DHCP service must be restarted. Issue “killall dhcpd” command to disable DHCP service and then issue “dhcpd” command to enable DHCP service.

Step 4. Backup a Configuration File

Before preparing a configuration file in TFTP/FTP Server, please make sure the device generating the configuration file is set to **“Get IP address from DHCP”** assignment. This is because that DHCP Auto-provisioning is running under DHCP mode, so if the configuration file is uploaded by the network type other than DHCP mode, the downloaded configuration file has no chance to be equal to DHCP when provisioning, and it results in MD5 never match and causes the device to reboot endless.

In order for your Managed Switch to retrieve the correct configuration image in TFTP/FTP Server, please make sure the filename of your configuration file is defined exactly the same as the one specified in in **dhcpd.conf**. For example, if the configuration image’s filename specified in dhcpd.conf is “metafile”, the configuration image filename should be named to “metafile” as well.

Step 5. Place a copy of Firmware and Configuration File in TFTP/FTP

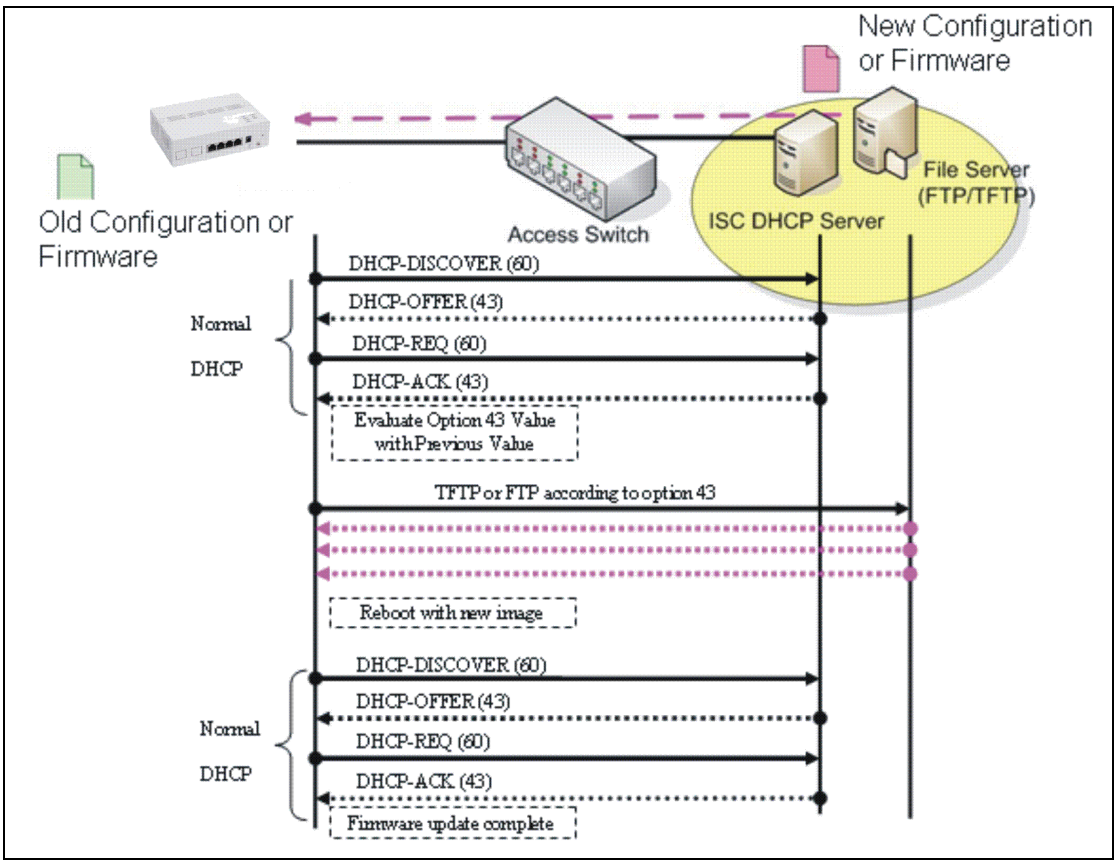
The TFTP/FTP File server should include the following items:

1. Firmware image (This file is provided by the vendor.)
2. Configuration file (This file is generally created by users.)
3. User account for your device (For FTP server only.)

B. Auto-Provisioning Process

This switching device is setting-free (through auto-upgrade and configuration) and its upgrade procedures are as follows:

1. The ISC DHCP server will recognize the device whenever it sends an IP address request to it. And ISC DHCP server will tell the device how to get a new firmware or configuration.
2. The device will compare the firmware and configuration MD5 code form of DHCP option every time when it communicates with DHCP server.
3. If MD5 code is different, the device will then upgrade the firmware or configuration. However, it will not be activated right after.
4. If the Urgency Bit is set, the device will be reset to activate the new firmware or configuration immediately.
5. The device will retry for 3 times if the file is incorrect, then it gives up until getting another DHCP ACK packet again.



This page is intentionally left blank.